(UPDATED) DECEMBER 2012

Drive-by downloads

1. Cyber adversaries are increasingly using drive-by download techniques to deliver malicious software that compromises agency networks. This document explains how drive-by downloads operate and how the risk of compromise from these techniques can be mitigated. This document is intended to assist Information Technology Security Advisers in protecting their networks.

What is a drive-by download?

2. A drive-by download occurs when a user visits a legitimate website that has been temporarily compromised, enabling an adversary to install malicious software on the user's computer. It occurs without the knowledge or authorisation of the user.

What happens in a drive-by download?

3. A drive-by download starts when a user goes to a legitimate but compromised website. When the user accesses the website, the cyber adversary's malicious code exploits weaknesses or other vulnerabilities in the user's browser or browser plug-ins, allowing the download of malicious files to the user's computer. The downloaded files could enable the adversary to have full access and control of the user's computer, either to steal valuable information or to launch denial of service attacks against other users on the Internet.

4. Another form of a drive-by download is "Malvertisement", which is commonly Flash Player based and takes advantage of unpatched software. Disguised as legitimate advertisers, cyber adversaries implant their malicious software in an advertisement on a legitimate website. When the victim views the advertisement, the malware will start to infect the victim's computer.

5. Most drive-by downloads require scripts to be loaded from third party sites. Cyber adversaries inject inline frame codes into a legitimate website, which will load malicious software hosted on another website operated by the adversaries when the website is visited.

6. Search Engine Optimisation (SEO) is another technique often used in conjunction with a drive-by download exploit. SEO increases a website's visibility in a search engine. Generally, the higher or more often a website appears in the search result, the more traffic the website is likely to receive from the search engine's users. Cyber adversaries use SEO to promote their malicious websites in search engines to increase the chance of getting traffic to their website for the exploit to occur.

7. There are malware kits available which target specific browser or software flaws, including Adobe PDF, Microsoft's Internet Explorer as well as other browser plug-ins. The server to which these kits are connected can use HTTP request headers from a browser, to determine which specific exploits are most likely to work on the victim's computer.

8. As of late October 2011, drive-by download sites have started using new techniques where they use complex logic to limit their attacks to previously uninfected networks[1]. The technique also attempts to avoid monitoring tools which blacklist compromised websites. Consequently, you should adopt a defence-in-depth approach to network security, instead of relying mainly on anti-virus programs.

Minimise the risk

9. To mitigate the risks of drive-by downloads, at least the top four strategies of DSD's *Strategies to Mitigate Targeted Cyber Intrusions* should be implemented in your environment. Other strategies may also be effective, depending on security gaps in your network.

10. The top four strategies involve:

a. Strategy 1: **Implementing application whitelisting**. In many cyber incidents witnessed by the Cyber Security Operations Centre, application whitelisting was the only strategy able to stop drive-by downloads from executing the malicious software.

b. Strategies 2 and 3: **Patching applications and operating system** vulnerabilities, especially Java and Flash. Old versions of a product are more vulnerable to these exploits. Keep all applications up to date.

c. Strategy 4: **Minimising the number of users with domain or administrator privileges**. Limit the ability for users with administrator privileges to have access to email and the Internet by employing separate unprivileged workstations or accounts for these purposes.

11. Agencies should also consider implementing these strategies from the remainder of the list:

a. Strategy 15: **Implement a robust web content filtering solution** that inspects the content of all web traffic for potentially malicious downloads and blocks them based on that inspection. Preferably disallow ActiveX, Java, Flash, HTML inline frames and javascript, except for whitelisted web sites.

b. Strategies 16 and 17: **Implement domain whitelisting for all domains including HTTPS/SSL domains**, to only enable trusted domains to be accessed by users. This will not prevent drive-by download attacks, but it will prevent secondary malicious websites from loading.

c. Strategy 25**: Install and maintain updated antivirus software** capable of scanning Internet traffic and detecting exploits.

[1] Sophos Naked Security Report "Analysis of compromised web sites hacked PHP scripts".

Further information

12. The *Australian Government Information Security Manual* (ISM) assists in the protection of official government information that is processed, stored or communicated by Australian Government systems:

http://www.dsd.gov.au/infosec/ism/index.htm

13. DSD's *Strategies to Mitigate Targeted Cyber Intrusions* and other DSD products complement the advice in the ISM. The complete list of mitigation strategies can be found at:

http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

Contact details

Australian government customers with questions regarding this advice should contact the DSD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or dsd.assist@defence.gov.au.

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.